Method for authentication by an external medium of a portable object such as a memory card coupled to this medium

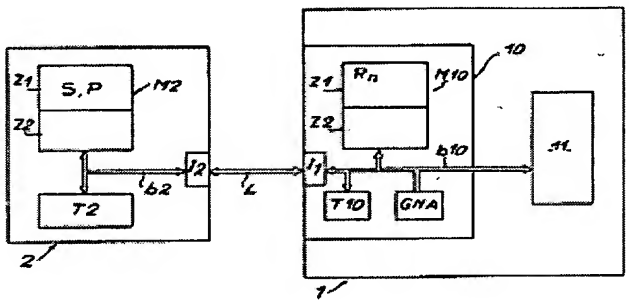
Patent number: JP8027822B
Publication date: 1996-03-21
Inventor: HAZARD MICHEL (FR)
Applicant: BULL CP8 (FR)
Classification:
- international: ***G07F7/10; H04L9/32;*** **G07F7/10; H04L9/32;** (IPC1-7): G06K17/00; G06F19/00
- european: G07F7/10D4E2; G07F7/10E; H04L9/32
Application number: JP19870503572 19870615
Priority number(s): WO1987FR00221 19870615; FR19860008654 19860616

Also published as:
EP0250309 (A1)
WO8707743 (A1)
US5153581 (A1)
FR2600189 (A1)
EP0250309 (B1)

Report a data error here

Abstract not available for JP8027822B
Abstract of corresponding document: **US5153581**

PCT No. PCT/FR87/00221 Sec. 371 Date Feb. 12, 1988 Sec. 102(e) Date Feb. 12, 1988 PCT Filed Jun. 15, 1987 PCT Pub. No. WO87/07743 PCT Pub. Date Dec. 17, 1987.A method for authentication by an external medium of a portable object such as a standardized credit card coupled to this medium. The portable object (2) calculates a result (R) which is at least a function of a secret key (S) and of a variable datum (E). This result (R) is sampled by the external medium (1), which compares it with a reference result (RO). This result (RO) is changed in a random manner, by being replaced by a new result (RO) calculated by a portable object (2) which has been authenticated based on the preceding reference result.



(19)日本国特許庁（ＪＰ）　(12)特　許　公　報（Ｂ２）　(11)特許出願公告番号

特公平8－27822

(24)(44)公告日　平成８年(1996)３月21日

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０６Ｋ　17/00		Ｔ		
Ｇ０６Ｆ　19/00				
			Ｇ０６Ｆ　15/ 30　３５０　Ａ	

発明の数１(全 5 頁)

(21)出願番号　特願昭62－503572

(86)(22)出願日　昭和62年(1987)６月15日

(65)公表番号　特表平1－502218

(43)公表日　平成１年(1989)８月３日

(86)国際出願番号　ＰＣＴ／ＦＲ８７／００２２１

(87)国際公開番号　ＷＯ８７／０７７４３

(87)国際公開日　昭和62年(1987)12月17日

(31)優先権主張番号　８６０８６５４

(32)優先日　1986年６月16日

(33)優先権主張国　フランス（ＦＲ）

審判番号　平5－20221

(71)出願人　999999999
ピュル　セーペー８
フランス国　78430　ルーヴシェンヌ、ペペ45，ルート・ドゥ・ヴェルサイユ　68

(72)発明者　アザール　ミシェル
フランス国　78124　マレイユ／モルドゥル　リュ　デ　アリア　27

(74)代理人　弁理士　湯浅　恭三　(外５名)

審判の合議体
審判長　菅野　嘉昭
審判官　内藤　二郎
審判官　赤穂　隆雄

最終頁に続く

(54)【発明の名称】　外部装置により携帯可能な物体の正当性を証明する方法

【特許請求の範囲】

【請求項１】外部装置（１）によりこの外部装置に接続された携帯可能物体（２）の正当性を証明するために、少なくともこの携帯可能物体（２）のメモリ（M2）に前もって記憶された秘密キー（Ｓ）と上記外部装置（１）から供給された変更可能な外部データ（Ｅ）との関数である結果（Ｒ）を上記携帯可能物体（２）の処理回路（T2）に計算させる形式の証明方法であって、上記外部装置（１）に以前に接続された携帯可能物体（２）により同一の上記変更可能な外部データ（Ｅ）から計算された少なくとも１つの以前の結果（Ra）と上記結果（Ｒ）とを比較することを特徴とする、外部装置により携帯可能な物体の正当性を証明する方法。

【請求項２】上記の変更可能なデータ（Ｅ）をもとにして参照用結果（R0）を計算し、この参照用結果（R0）を

上記外部装置（１）のメモリ（M10）に記憶させ、上記携帯可能物体（２）により計算された各結果（Ｒ）が、この参照用結果（R0）と必ず等しいことを特徴とする請求項１に記載の、外部装置により携帯可能な物体の正当性を証明する方法。

【請求項３】許可された人が所持する参照用携帯可能物体（2a）を用いて上記参照用結果（R0）を計算させることを特徴とする請求項２に記載の、外部装置により携帯可能な物体の正当性を証明する方法。

【請求項４】携帯可能物体をｎ回接続した後に上記の変更可能なデータ（Ｅ）を変更し、ｎ自体も変更可能であることを特徴とする請求項１または２に記載の、外部装置により携帯可能な物体の正当性を証明する方法。

【請求項５】上記外部装置から供給された新しい変更可能なデータ（Ｅ）をもとにして、以前の参照用結果に基

づいて正当であると判定されたばかりの携帯可能物体（２）を用いて、新しい参照用結果（R0）を計算させることを特徴とする請求項４に記載の、外部装置により携帯可能な物体の正当性を証明する方法。

【請求項６】上記外部装置（１）のランダム数発生器（GNA）から上記の変更可能なデータ（E）を得ることを特徴とする請求項１～５のいずれかに記載の、外部装置により携帯可能な物体の正当性を証明する方法。

【発明の詳細な説明】

本発明は、外部装置により、携帯可能な物体、例えばこの外部装置に接続されたメモカードの正当性を証明する方法に関するものである。

特に、本発明は、外部媒体がカードを介してシステムに制御命令を供給するとかシステムにアクセスする許可を与える機能を有するが、所定のカードだけがこの外部媒体と連動できるようにオーソライズされているため、この外部装置に接続されたカードが制御命令の供給またはアクセス許可の権利が本来あるかどうかを、この外部装置が前もってはっきりと確認する必要がある場合に応用される。。

一般に、カードなどの携帯可能物体を利用する場合には、たいてい用途ごとに少なくとも１つの特定の秘密キーが利用される。このキーは、所定の用途にアクセス可能な全カードに前もって記憶されるとともに、この用途において制御命令を供給する、またはアクセス許可を与えるためにこのカードに接続される可能性のある全装置にも記憶される。秘密キーは、カードを発行しており、かつ、このカードと連動する装置を管理する許可を与えられた機関のみに知らされている。どの用途でも、装置は、この装置自体が記憶している秘密キーがカードの秘密キーと確かに一致していることを、秘密キーの値を明らかにすることなく確認する必要がある。

一般に、この確認作業はカードと装置の間の情報交換による対話という形態で行われる。このことは、例えば本特許出願の出願人のフランス国特許第2469,760号に記載されている。

この特許によると、対話は以下のように行う。すなわち、ランダムな数値を外部からカードに１つ入力し、カードの処理回路で計算を実行させて、このランダムな数値と前もって記憶されている秘密キーの関数である結果を導出し、この結果をカードから出力させ、この結果を装置による計算結果である少なくとも上記のランダムな数値とこの装置に前もって記憶されている秘密キーの関数である結果と比較する。

このカード確認操作またはカードの正当性の証明操作は、上記の２つの結果が一致している場合に終了する。もちろん、秘密キーが互いに等しい場合にしかこのような一致は得られない。

不正者が不正カードを製造することが絶対にできないようにするためには、特に一般人がアクセスできる装置

の段階で、使用されるキーの秘密が保持される必要がある。一般に、キーはメモリ領域に記憶され、次いで外部からアクセスできないようにロックされる。このメモリ領域には、このメモリ領域に接続された処理回路を通して内部からしかアクセスすることができない。しかし、不正行為は可能性が低く技術的に難しいとはいえ、常に可能であることを認めなくてはならない。不正者は、例えばキーが記憶されたメモリをレーザで読出す方法などの進んだ方法で秘密キーを発見しようとする。

この課題を解決するため、本発明は、秘密キーの代わりに時間経過とともに変化する情報を装置に記憶させる一方、この装置が、連動する可能性のあるカードの正当性を証明できるようにするものである。

つまり、本発明によれば、外部装置によりこの外部装置に接続された携帯可能物体の正当性を証明するために、少なくともこの携帯可能物体のメモリに前もって記憶された秘密キーと上記外部装置から供給された変更可能データの関数である結果を上記携帯可能物体の処理回路に計算させるタイプの証明方法であって、上記結果と、上記外部装置に以前に接続された携帯可能物体により同じ上記変更可能データから計算された少なくとも１つの以前の結果とを比較することを特徴とする方法が提供される。

本発明の別の特徴によれば、使用される上記の変更可能データは、外部装置により正当性が証明されたばかりの携帯可能物体によりランダムに変更される。

本発明の重要な特徴によれば、外部装置となる装置はすべてありふれた装置であり、機密情報または秘密情報をまったく記憶していない。

上記した以外の特徴、利点および詳細は、実施例を示す添付の図面を参照して行う以下の説明により明らかになろう。

第１図は、本発明の方法を実行するシステムの第１の実施例の概略図である。

第２図は、本発明の方法を実行するシステムの第２の実施例の概略図である。

第１図のシステムは、装置またはターミナル１として簡単化して表した外部媒体と、携帯可能物体２とで構成されている。携帯可能物体２は、所持者が例えば別のシステム（図示せず）に対する制御命令の供給を受ける、またはアクセス許可を得ることができるように一時的に装置１に接続される。

装置１は、制御装置10と、目的とする用途に応じた装置にそれぞれ対応する回路群11とに分かれている。

制御装置10は、メモリM10と、処理回路T10と、ランダム数値発生器GNAとに分かれている。これら３つの要素は、すべて制御・データ・アドレス用バスb10を介して回路群11に接続されている。メモリM10は少なくとも２つのメモリ領域１とZ2に分けられている。メモリ領域Z1は、一旦書込まれると処理回路T10によってしかアクセ

スできないデータを記憶する。これに対してメモリ領域Z2は、読出しのときに外部からアクセスが可能であり、読出し／書込みのときに処理回路T10によってアクセスが可能なデータを記憶する。

携帯可能物体２は例えばメモリM2と処理回路T2を備えたメモリカード（ICカード）である。メモリM2はプログラム可能なメモリである。また、処理回路T2は例えばマイクロプロセッサである。メモリM2と処理回路T2は、制御・データ・アドレス用バスb2を介して互いに接続されている。カードのメモリM2はやはり少なくとも２つの領域Z1とZ2に分けられている。それぞれの領域へのアクセス条件は装置１のメモリM10の場合と同様である。このタイプのカードは、特に、本特許出願の出願人のフランス国特許第2,401,459号と第2,461,301号に記載されている。

カード２と装置１の接続は、装置１側はインターフェイスI1により、カード２側はインターフェイスI2により行われる。この２つのインターフェイスは、近距離または遠距離を接続線Ｌにより相互に接続されている。このような接続装置は、特に、本特許出願の出願人のフランス国特許第2,483,713号に記載されている。

カード２のメモリM2のメモリ領域Z1には、このカード２から得られる制御命令に専用の秘密キーＳが記憶されている。

本発明によれば、秘密キーＳが記憶されているカード２と連動する装置１にはいかなる秘密キーＳも記憶されていない。

第１図の実施例に従って、この場合でも、装置１に接続されており秘密キーＳが記憶されたカード２の正当性をこの装置１が証明可能であることを説明する。

装置１はカード２にランダムな数値Ｅを送る。カード２の処理回路T2はメモリ領域Z1に前もって記憶されているプログラムＰを実行する。このプログラムＰは、少なくとも上記のランダムな数値Ｅと秘密キーＳを考慮して、以下の式

$R = f\ (E, S)$

で表される結果Ｒを計算する。

このようにして得られた結果は次に装置１の制御装置10に送られて解析され、カード２の有効性が判定される。

このためには、ｎ枚のカード２が既に装置１に接続されたことがあると仮定する。これらｎ枚のカードはｎ個の計算結果Raを既にそれぞれ計算して制御装置10のメモリ領域Z1に次々と記憶させている。ここでさらに、これらｎ個の計算結果がすべて同一のランダムな数値Ｅから計算されたものと仮定する。ところで、ランダムな数値Ｅは、発生器GNAから出力された後に制御装置10のメモリM10のメモリ領域Z2に記憶されている。

カード２の正当性の確認は、結果Ｒをそれ以前の結果Raと比較することにより行う。実際には、４つの場合が考えられる。

最初の２つの場合には、以前の結果Raがすべて同じであると仮定されている。すなわち、以前の結果Raはすべて、同一の用途に対する同一の秘密キーＳを記憶しているカードにより同一のランダムな数値Ｅから計算されたものである。

第１の場合には、結果Ｒはそれぞれの結果Raと等しい。すると制御装置10はカード２が正当なものであると判断して、装置Ｒを記憶させる。次にこの結果Ｒは古い結果Raとなって装置１に回路群11の作動を許可する制御信号を発生させる。

第２の場合には、結果Ｒがそれぞれの結果Raと異なる。すると制御装置10はカード２が不正なものであると判断して回路群11の作動を禁止する。

第３の場合と第４の場合には、以前の結果Raは必ずしもすべてが互いに等しくはないと仮定されている。すなわち、以前の結果Raは異なった用途に対する異なった秘密キーＳから計算されたものである。

上記の各場合には、各カード２により計算された様々な結果Ｒが制御装置のメモリM10に記憶されている。メモリを節約するためには同じ結果を重複しては記憶させないで、異なった結果が現れた最初のときにその結果Ｒを記憶させるとともに、カウンタを用い、新しい結果Ｒが既に記憶された結果と同じであるときにはそのたびごとにこのカウンタをインクリメントするのが好ましい。

利用者のカード２ごとにさらにモニタ操作を行うことにより、同一のカード、特に不正なカードがｎ回連続して装置１に接続されることがあっても、この装置１が騙されて、カード２により計算されたすべて同一の以前の結果Raが正当で、ｎ枚の異なる正当なカードから得られたものであると判定することがないようにするのが好ましい。このモニタ操作は、カード所持者に固有のデータ、例えばカードのシリアル番号を装置１に記憶させ、同一のカードがこの装置に接続された回数をモニタすることにより行う。

このような構成にすると、参照用の結果Ｒがまだ外部装置１に記憶されていない時、あるいは記憶されている参照用結果Raの種類が極めて少ない場合に、携帯可能な物体２を最初に挿入したとき外部装置がどのように動作するかを設計する際に、次に二つの可能性が考えられる。

（ａ）挿入される携帯可能な物体２に対応する以前の結果が記憶されていない場合、携帯可能な物体によって送られたいづれの結果も正しい、と判断するように設計する、あるいは、

（ｂ）以前の結果が記憶されていない場合、送られた結果はすべて誤りであり、この場合、いかなる物体の正当性も証明されない、と判断する、

という以上の二つである。

いずれにしても、このままでは最初のユーザに対して

はそのカードの正当性を検証することは不可能である。

この問題は、第２図に示した第２の実施例のようにして、この装置１を管理する許可を与えられている機関が先ず参照用の結果R0を書き込むようにすることによって解決される。この図の装置１では、この装置１を管理する許可を与えられている機関が使うことのできる参照用カード2aに記憶されている特定の用途に対応する秘密キーＳを用いて参照用結果R0が計算される。そしてこの参照用結果R0が、この機関が提供する特定の用途を利用するために装置１にアクセス可能な全カードに共通な同一の秘密キーＳに対する最初の参照用結果として外部装置１のメモリM10のメモリ領域Z1に記憶される。

第２図の参照用カード2aは第１図のカード２と同じタイプのカードである。許可を得た人がこの参照用カード2aを装置１に接続すると、この装置１内のランダム数値発生器GNAはランダムな数値Ｅを出力して参照用カード2aに送る。参照用カード2aの処理回路T2は、結果Ｒの計算の場合と同様にして参照用結果R0を計算する。この参照用結果R0は制御装置10のメモリM10のメモリ領域Z1に記憶される。次に、カード２で計算された各結果Ｒがこの参照用結果R0とだけ比較される。この場合、制御装置のメモリM10に様々なカード２により計算された結果を記憶させる必要はない。

本発明の重要な特徴によると、ランダムな数値Ｅは安全のために変更することができる。この変更は定期的に実行するのではなく、例えば装置にｎ枚のカードが接続された後に行う。この数ｎは変えることができる。ラン＊

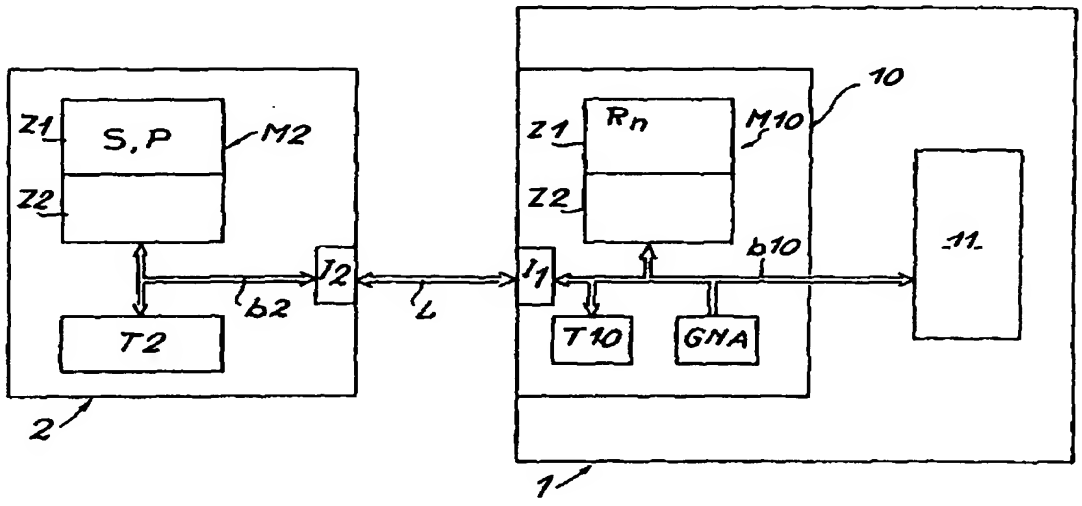
＊ダムな数値Ｅを変更するということは、新しい参照用結果R0を計算することを意味する。この計算を行うためには、初期化のために以前に用いた参照用カード2aを用いることができる。この解決法は十分なものではない。というのは、変更のたびごとに、この参照用カード2aの所持を許可された人が各装置１のところに出かけることを意味するからである。

本発明では、まったく簡単に、以前の参照用結果R0をもとにして正当であると判定された利用者のカード２により新しい参照用結果R0を計算する。従って、参照用カード2aを用いる必要がない。

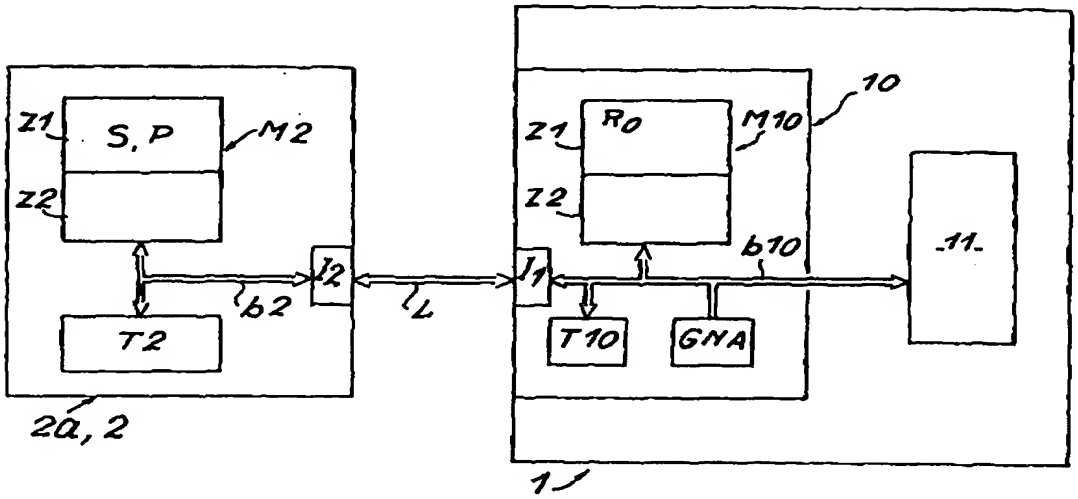
さらに詳しく説明すると、ｎ番目のカード２（ｎは変更可能）が正当であると判定されると、装置１のランダム数値発生器GNAがランダムな数値Ｅをカード２に出力する。するとこのカード２のマイクロプロセッサT2が新しい参照用結果R0を計算する。次に、この参照用結果R0のほか、出力されたばかりのラダムな数値Ｅが装置１のメモリM10に記憶される。

本発明の装置１を用いると、カード２の正当性をこれらカードに記憶された秘密キーＳに基づいて確認することができる。しかも、秘密キーを知る必要がなく、再計算する必要もない。このときに確認されるのは、同一の秘密キーを有するカードのみであ。また、複数の異なる秘密キーＳに対応する複数の結果を装置１から発生させ、複数種のカードの正当性を判定することが可能である。この場合、それぞれの種類のカードは装置１で確認可能な所定の秘密キーを記憶している。

【第１図】



【第２図】



フロントページの続き

(56)参考文献　特開　昭59－77575（ＪＰ，Ａ）
特開　昭60－181891（ＪＰ，Ａ）
特開　昭59－139479（ＪＰ，Ａ）
米国特許3798605（ＵＳ，Ａ）
米国特許4471216（ＵＳ，Ａ）